

EXHIBIT 11

1/31/25, 12:00 PM

Google Workspace Updates: Block compromised mobile devices using context-aware access

Google Workspace Updates

This official feed from the Google Workspace team provides essential information about new features and improvements for Google Workspace customers.

1/31/25, 12:00 PM

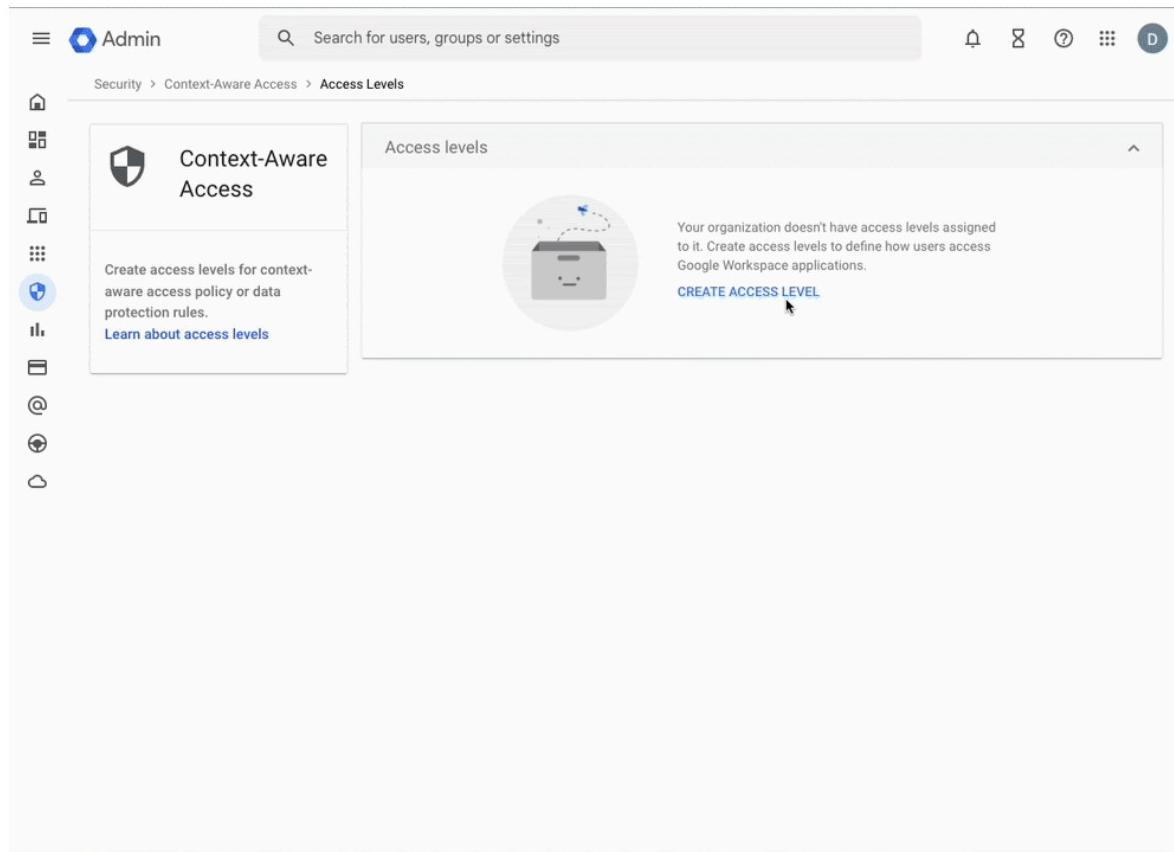
Google Workspace Updates: Block compromised mobile devices using context-aware access

Block compromised mobile devices using context-aware access

Monday, May 6, 2024

What's changing

Using context-aware access, you now have the option to automatically block access to Google Workspace data from compromised Android and iOS devices. A device may be counted as compromised if certain unusual events are detected, including devices that are jailbroken, bypassing of security controls, modification of restricted settings, and more.

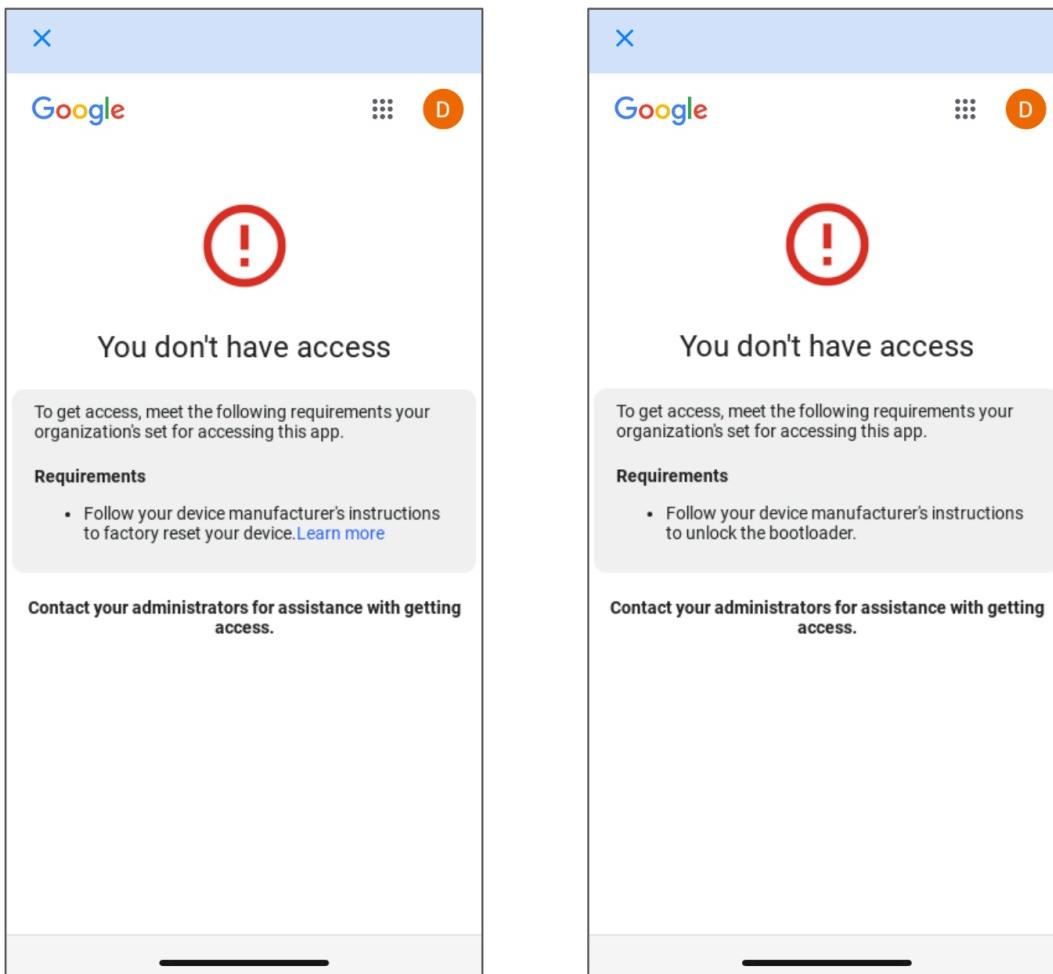


The screenshot shows the Google Workspace Admin console interface. The left sidebar has icons for Home, Users, Groups, Roles, Data Protection, Admin, and Help. The main navigation bar at the top says "Admin" and includes a search bar and various status indicators. Below the navigation, the path "Security > Context-Aware Access > Access Levels" is shown. On the left, there is a card for "Context-Aware Access" with a shield icon, instructions to "Create access levels for context-aware access policy or data protection rules.", and a link to "Learn about access levels". To the right, under "Access levels", there is a placeholder message: "Your organization doesn't have access levels assigned to it. Create access levels to define how users access Google Workspace applications." Below this message is a blue button labeled "CREATE ACCESS LEVEL" with a cursor pointing to it. The overall theme is light gray with blue highlights for interactive elements.

Creating a new rule to block compromised mobile devices

1/31/25, 12:00 PM

Google Workspace Updates: Block compromised mobile devices using context-aware access



Blocking message for compromised iOS and Android devices

Getting started

- **Admins:** Visit the Help Center to learn more about how to create context conditions and apply rules with compromised device signals, and our Developer documentation regarding custom access level specification. Compromised device events reports can be viewed in the security center by going to Security > Security center > dashboard > compromised device events.

Rollout pace

1/31/25, 12:00 PM

Google Workspace Updates: Block compromised mobile devices using context-aware access

- **Block access to Google Workspace data:** available immediately for both Android and iOS.
- **Remediation message:** available immediately for Android, available on May 9, 2024 for iOS.

Availability

Available to Google Workspace

- **Enterprise Standard and Plus**
- **Education Standard and Plus**
- **Frontline Standard**
- **Enterprise Essentials Plus**
- **Cloud Identity Premium**

Resources

- [Google Workspace Admin Help: Set up Context-Aware Access](#)
- [Access Context Manager Help: Custom access level specification](#)
- [Google Workspace Admin Help: Compromised device events report](#)



Labels: [Admin console](#) , [MDM](#) , [Rapid Release](#) , [Scheduled Release](#) , [Security and Compliance](#)



1/31/25, 12:00 PM

Google Workspace Updates: Block compromised mobile devices using context-aware access



[Google](#) · [Privacy](#) · [Terms](#)